Fortinet FortiAnalyzer Virtual Appliance for Microsoft Azure Quick Start Guide

FORTINET FORTIANALYZER VIRTUAL APPLIANCE FOR MICROSOFT AZURE QUICK START GUIDE

The following section will take you through a step-by-step process in order to deploy Fortinet FortiAnalyzer on Azure.

What is Fortinet FortiAnalyzer for Azure?

Networks are constantly evolving due to threats, organizational growth, or new regulatory/business requirements. Traditional analysis products focus on recording and identifying company-wide threats through logging, analysis, and reporting over time.

FortiAnalyzer offers enterprise-class features to identify these threats, but also provides flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements while aggregating logs in a hierarchical, tiered logging topology.

FortiAnalyzer platforms integrate network logging, analytics, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine-tune your policies. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, contents archiving, data mining, and malicious file quarantining.

Why Fortinet FortiAnalyzer on Azure?

Fortinet FortiAnalyzer deploys into Azure to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location, providing a simplified, consolidated view of your security posture. In addition, FortiAnalyzer provides detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

Key Features and Benefits

1. **Graphical Summary Reports** provide network-wide reporting of events, activities, and trends occurring on FortiGate® and third-party devices.
2. **Network Event Correlation** allows IT administrators to quickly identify and react to network security threats across the network.
3. **Scalable Performance and Capacity**—FortiAnalyzer supports thousands of FortiGates and can dynamically scale storage based on retention/compliance requirements.
4. **Choice of Standalone, Collector, or Analyzer Mode** allows deployment of individual instance or optimized for a specific operation (such as store and forward or analytics).
5. **Seamless Integration with the Fortinet Product Portfolio** enables tight integration to allow FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.

How to Deploy Fortinet FortiAnalyzer in Microsoft Azure Using the Azure Portal

The Fortinet FortiAnalyzer for Microsoft Azure is deployed as a virtual machine in Microsoft's Azure cloud (IaaS). You will see in the following sections how to deploy and configure the Fortinet FortiAnalyzer in the Azure Marketplace.

- Fortinet FortiAnalyzer 14-Day Trial.
- Fortinet FortiAnalyzer (BYOL)—This is currently the only licensing model that is supported. Fortinet also offers a 60-day evaluation license. https://support.fortinet.com/Evaluation/Login.aspx

BEFORE YOU GET STARTED

Before you can begin to deploy Fortinet's FortiAnalyzer for Azure, you will need to make sure the following conditions have been met in order to successfully complete the installation.

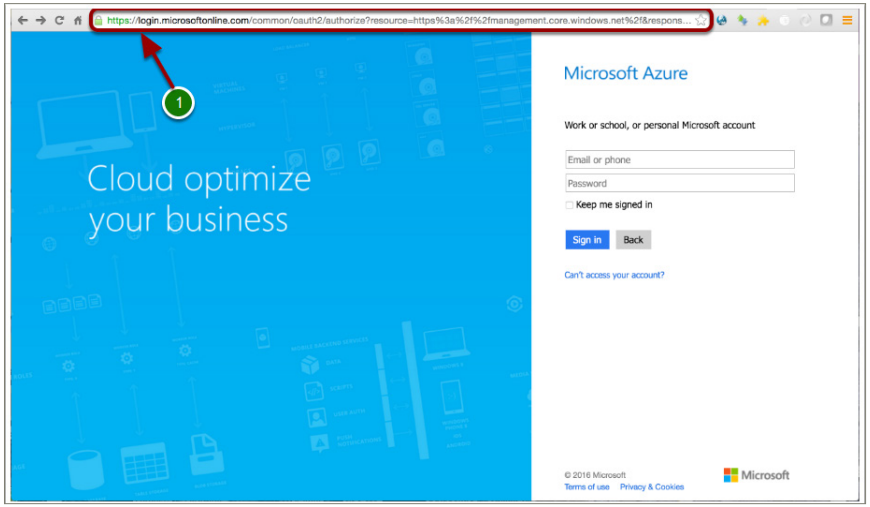
- Create a Microsoft Azure account
- Obtain a license (choose one of the following):
    1. Purchase a Fortinet FortiAnalyzer license for Microsoft Azure http://www.windowsazure.com/en-us/account/
    2. Register to receive an evaluation license from Fortinet https://support.fortinet.com/Evaluation/Login.aspx

Step-by-Step Instructions to Get the Fortinet FortiAnalyzer Up and Running on Azure

The following section will take you through a step-by-step process in order to deploy Fortinet FortiAnalyzer on Azure.

1. Log In to the Azure Portal
   - You can access the Azure portal using the following URL: https://portal.azure.com/
   - You will then be redirected to: https://login.microsoftonline.com/ (abbreviated URL due to its length)

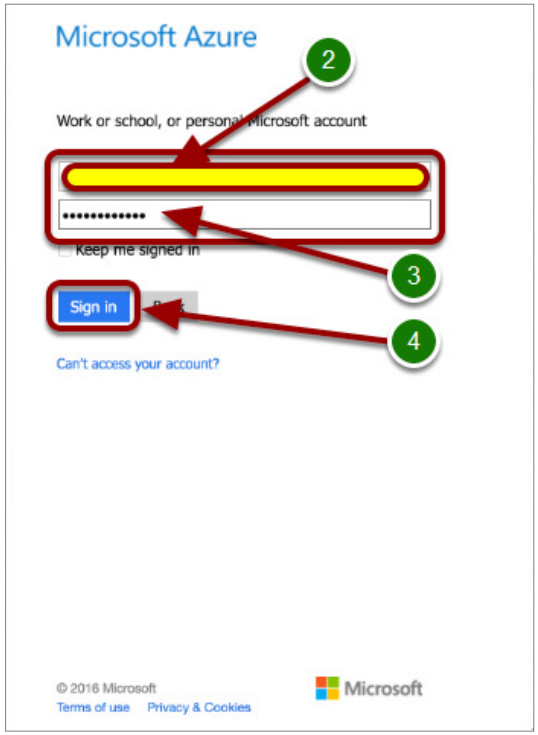
   The current Azure portal is the portal through which you will start creating and managing Azure services, such as the Fortinet FortiAnalyzer Virtual Appliance. The Azure portal includes a dashboard that you can configure to work with and monitor the resources in your environment. The Azure portal lets you administer all of your Azure platform resources in a single location. The current Azure portal uses ARM, although some classic model functionality is exposed through the new portal. The legacy or classic portal still is available for use, but the new portal has been released for general availability and is the portal you should use.



2. Enter User Credentials and Sign In

   Enter your user credentials:

   - Username: <Your Username> (2)
   - Password: <Your Password> (3)
   - Click "Sign in." (4)

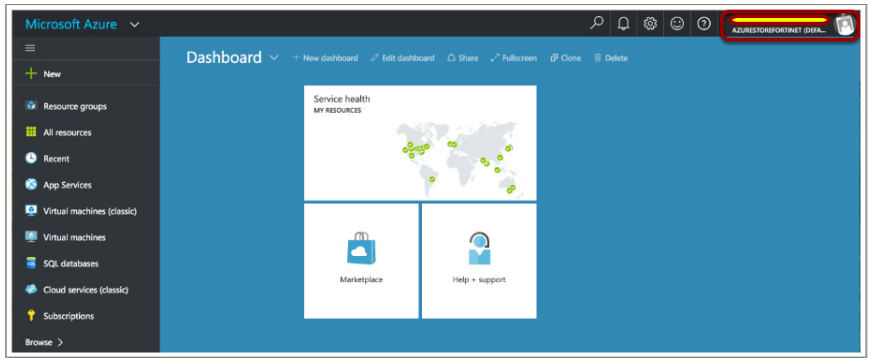


3. Successful Login to Azure

   Once you have successfully logged in to the Azure portal, you will observe the Microsoft Azure Dashboard.

   Note the following login details in the top right-hand corner of the Microsoft Azure Dashboard. If you click here, you will see options to:

   - Sign out
   - Change your password
   - View your permissions
   - View your bill

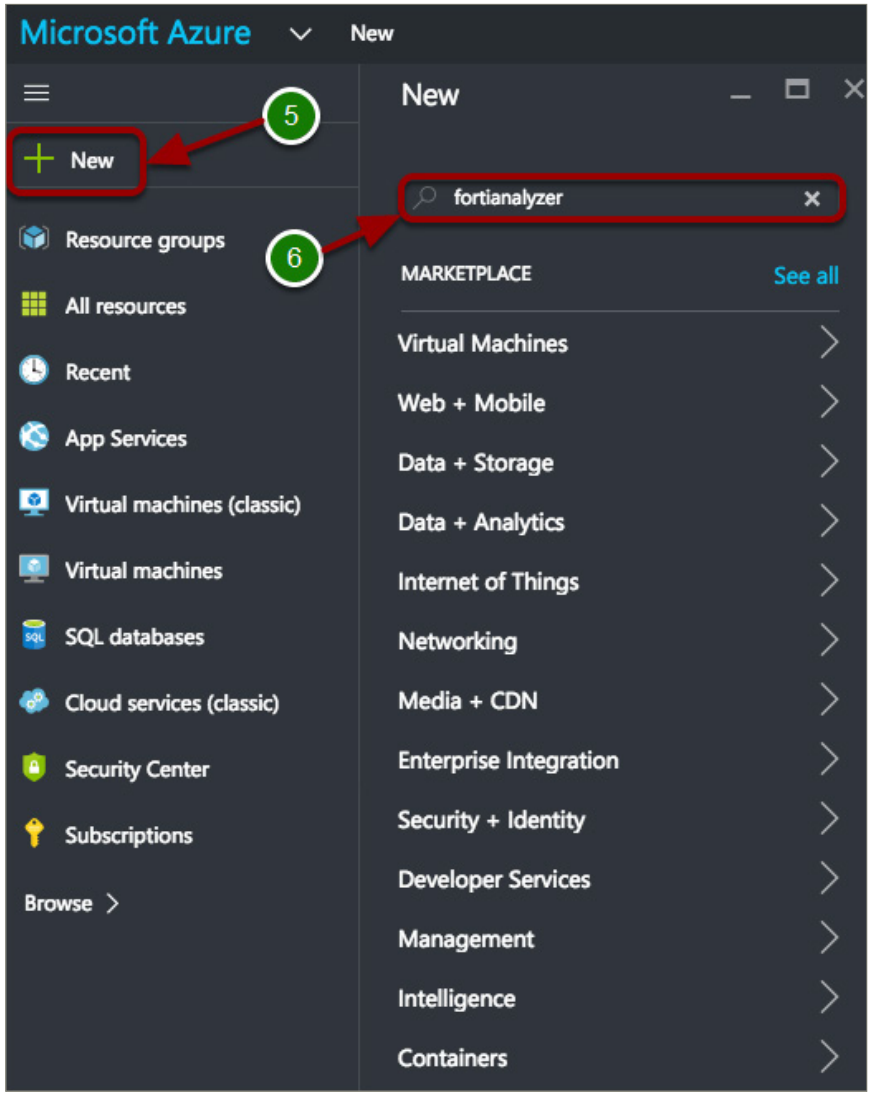


4. Creating the NEW Fortinet FortiAnalyzer in the Azure Marketplace

   In the Microsoft Azure portal, follow these steps:

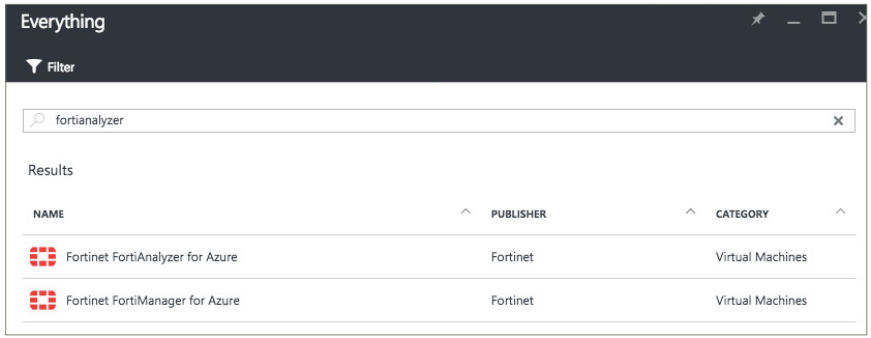
   - In the upper left-hand corner, click New (5).
   - In the New column, enter fortianalyzer in the "search the marketplace" and enter Return (6).

   NOTE: There are alternative ways of achieving the above; this is just one example.



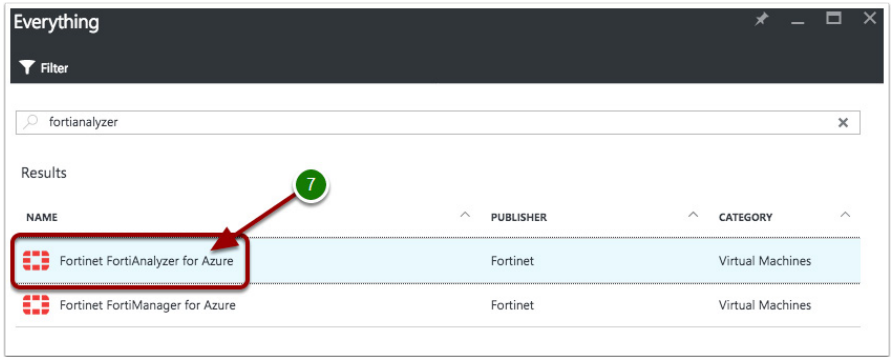
5. Fortinet Virtual Appliances Available in the Azure Marketplace

   You will now see something similar to this, which depicts the return of the “fortianalyzer” search results.



6. Select the Fortinet FortiAnalyzer for Azure from the Azure Marketplace

   Select Fortinet FortiAnalyzer for Azure (7).



7. Select the Fortinet FortiAnalyzer Deployment Model

   Once you have selected the Fortinet FortiAnalyzer VM, you will automatically be taken to the Resource Manager Panel, where you can create a deployment model.

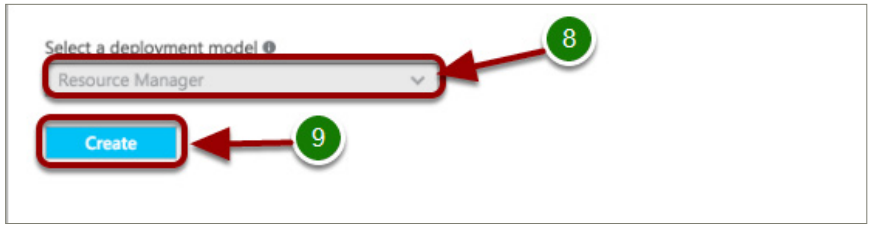
   - In Select a deployment model, select the default Resource Manager (8).
   - Then click Create (9).

   NOTE: Though there is no option from the dropdown menu to select a different deployment model, this is where you would select the Classic deployment model option.

   So what exactly are the Azure deployment models?

   Azure provides two deployment models, the Classic model and the Azure Resource Manager (ARM) model. The foundation of each model is an application-programming interface (API), which is the Resource Manager API for ARM and the Service Management API for the classic model. Although developers can write software to interact with these APIs directly through the REST API, it is more common to interact with these APIs indirectly using the Azure portal, the Azure PowerShell on Windows, or the Azure Command-Line Interface (CLI) on a Windows, OS X, or Linux computer.

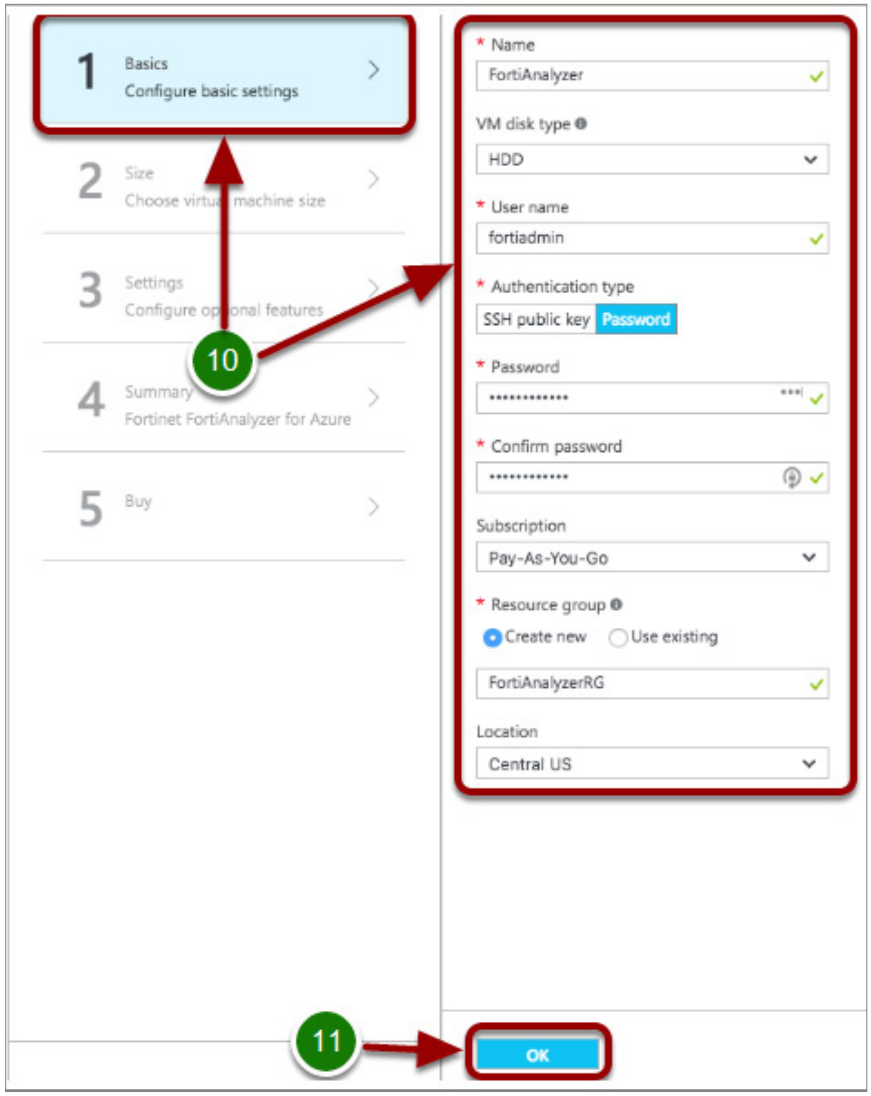
   In contrast to common belief, these two models are compatible with each other, but ARM simplifies the deployment and management of resources by managing them as a single resource group. Most newer resources support ARM, and eventually all resources will. However, how you create, configure, and manage Azure resources is different in these two models.



8. Configuring the FortiAnalyzer VM Basic Settings

   In the Configure basic settings panel (10), enter:

   - **FortiAnalyzer VM Name**—Enter the name of the FortiAnalyzer Virtual Appliance. (Only alphanumeric characters are permitted, and the value must be between 1 and 15 characters.)
   - **FortiAnalyzer Administrative Username**—Enter the administrator username for the FortiAnalyzer Virtual Appliance. (The administrator username for the FortiAnalyzer Virtual Appliance can NOT be "admin".) If you do enter "admin," you will get an error message stating that the specified username is NOT allowed. In addition to this, the username can NOT contain special characters.
   - **Authentication type**—Change Authentication type to Password.
   - **FortiAnalyzer Password**—Enter the administrator account password for the FortiAnalyzer Virtual Appliance. (The administrator account password MUST be between 6 and 72 characters, and MUST contain characters from at least three of the following groups: uppercase characters, lower case characters, numbers, and special characters.)
   - **Confirm password**—Re-enter the administrator account password for the FortiAnalyzer Virtual Appliance.
   - **Subscription**—The only available subscription for the FortiAnalyzer Virtual Appliance in Azure is the Pay-As-You-Go subscription model, so just leave this as the default.
   - **Resource group**—Enter the Resource group name, and note that only alphanumeric characters, periods, underscores, hyphens and parentheses may be used. In addition to this, a Resource group name can NOT end with a "." (With Azure Resource Manager, everything you provision on Azure is a resource. You can put multiple resources into a resource group. Managing resource groups and creating and updating resource groups are the most common operations using Azure Resource Manager.)



- **Location**—Select a location from the drop-down menu. The location refers to allowing you to administer all of your Azure platform resources in a single location.

Once you have confirmed that all the above settings are correct, click "OK" (11).

NOTE: If any of the values are incorrectly defined, you will see a "Red **!**"; otherwise, you will see a "Green ✓."

9. Configuring the FortiAnalyzer VM - Size

In the Azure Marketplace, the FortiAnalyzer virtual machines come in a variety of sizes, beginning with the A0 Standard up through the DS15_V2 with up to 20 cores. Each virtual machine size within each series has different limits for the amount of memory, number of NICs, maximum number of data disks, size of cache and maximum IOPS, and bandwidth.

Select the virtual machine size settings (12).

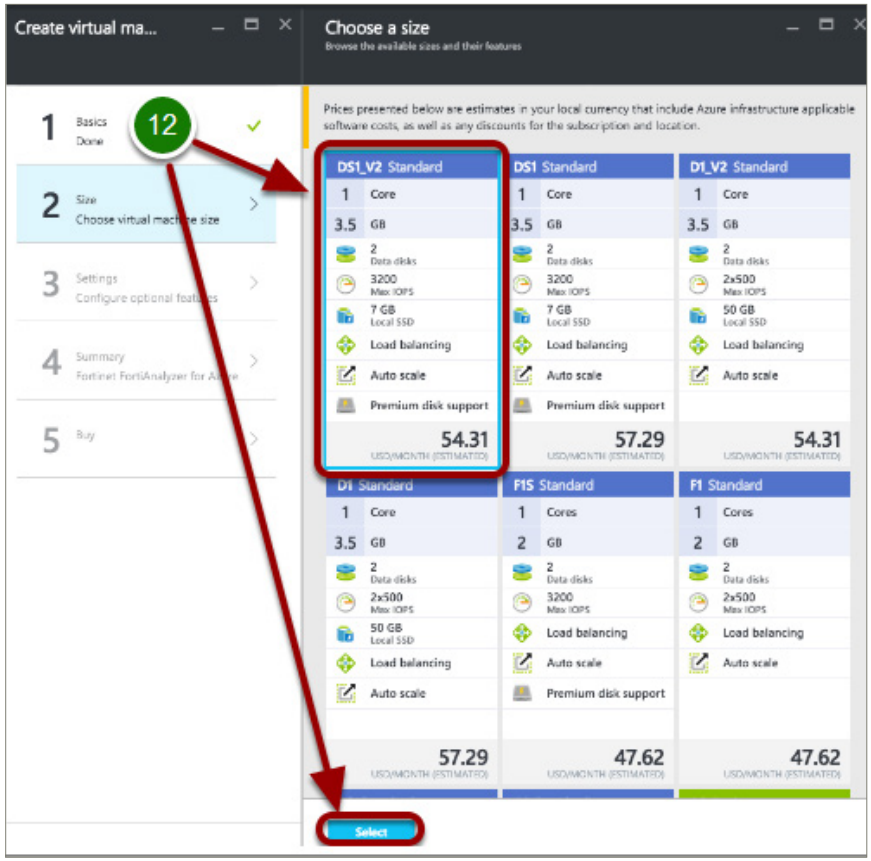
So what is “A4 Standard” and “D4 Standard?” Number of vNICs? What would be the use case for selecting the particular “virtual machine size?” Where can you find more guidance, so when you are selecting and setting this up, you can be more informed?

The “A4 Standard” and “D4 Standard,” etc., are what are referred to as instance sizes. The instances are differentiated primarily on CPU and memory, although they also have different levels of support for multiple vNICs. For more information, please click on the following URL:

https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-sizes/

But wait! When you select a “virtual machine size,” why do you not see the number of vNICs? From the “choose a size” panel, you have no idea and would have to guess. The answer is that Azure has never prioritized multiple vNICs. So, the Azure Marketplace templates have a bias against them, and it’s extremely difficult to create a variable number of vNICs. Fortinet’s FortiAnalyzer template facilitates the creation of one vNIC.

If you require more than one vNIC, you will need to deploy a custom template at this point. Please contact the Azure team (azuretech@fortinet.com) for assistance.



10. Configuring the FortiAnalyzer VM - Settings

    Below you will find your virtual machine settings. It is important to note:

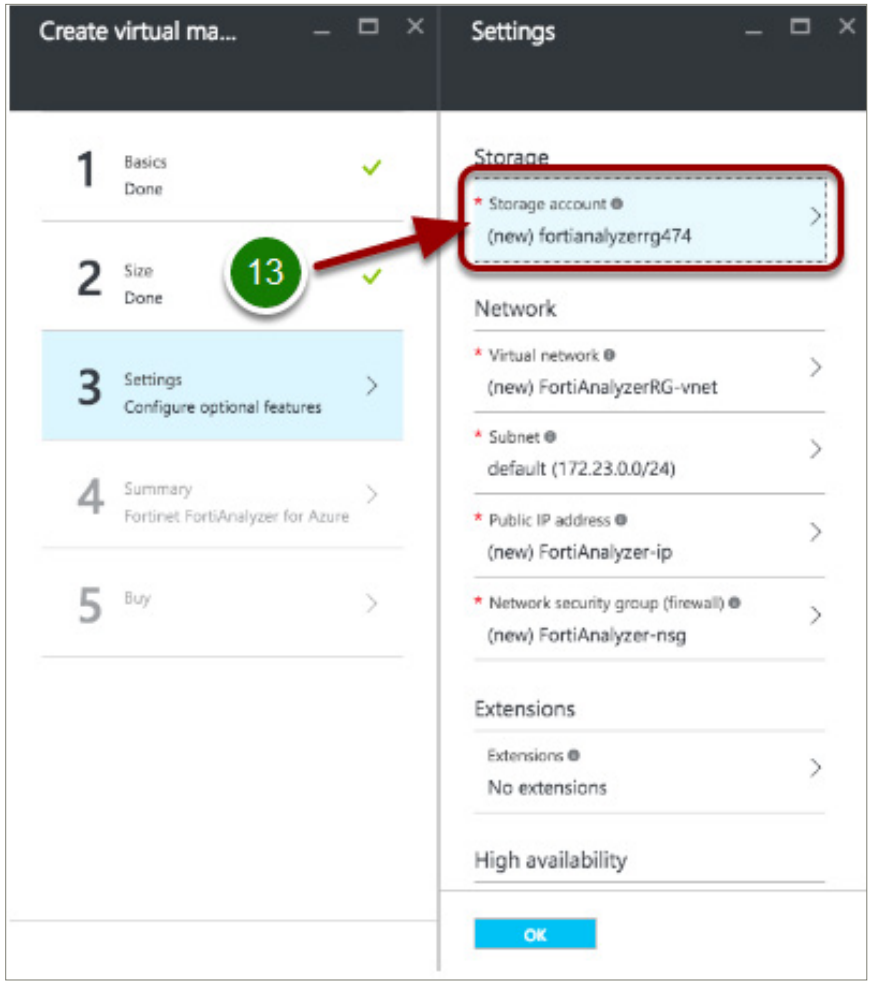
    - Storage account
    - Virtual network
    - Subnet
    - Public IP address, etc.

    These can all be customized. You could for example change your VNET to 10.0.0.0/8 and select for subnet 10.0.0.0/24. At this time you could receive warnings of overlapping address space in different resource groups within your locations; however, this doesn't matter and they don't cross-connect.

    For purposes of clarity, you will use default values for Standalone FortiAnalyzer QSG.

Configuring the FortiAnalyzer VM Settings - Storage Account

Our first option for settings is Storage (13). Through the Storage workflow you can accept the default storage account associated with the newly created resource group, or you can select another storage account if one previously exists.



Without going into the details of the different types of storage available in Azure, it is important to note (there are few exceptions) that all storage types are created from an Azure Storage Account. The Azure Storage Account in turn determines certain characteristics for the storage, such as whether the storage is locally redundant or geo-redundant, and whether the storage is based on standard HDDs or SSDs.

You can either create a new storage account or select an existing one for the FortiAnalyzer Virtual Appliance, but all resources should be in the same location (in this example: West Europe).

Select the Storage account settings (14).

Enter a Storage Account Name (15). (This account name can contain lowercase characters and numbers, and must be between 3 and 24 characters.)

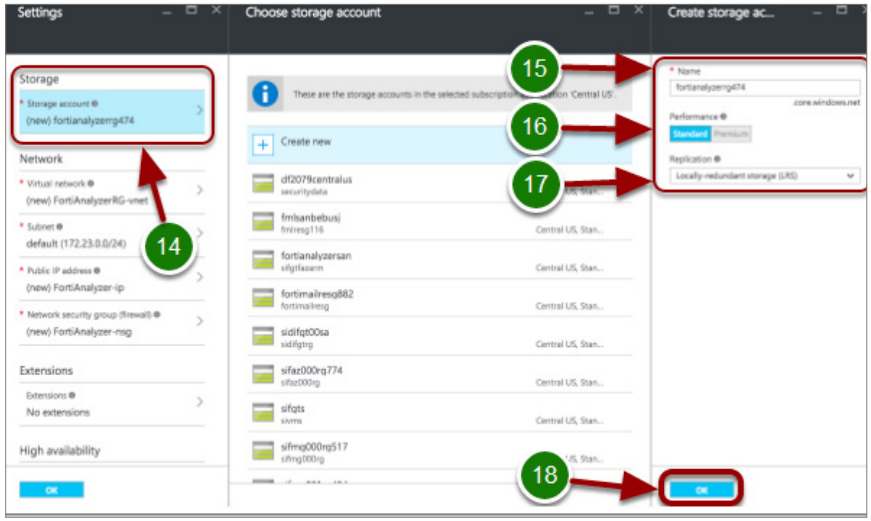
Select the Performance (16). (In this instance only standard is available.)

Select the Replication option you wish to use (17). There are two options available:

- Locally redundant storage (LRS)
- Geo-redundant storage (GRS)

Locally redundant storage (LRS) is where all data in the Azure Storage Account replicates synchronously to three different storage nodes within the primary region that was chosen when creating the Azure Storage Account.

Geo-redundant storage (GRS) is where every entity is replicated into two data centers.



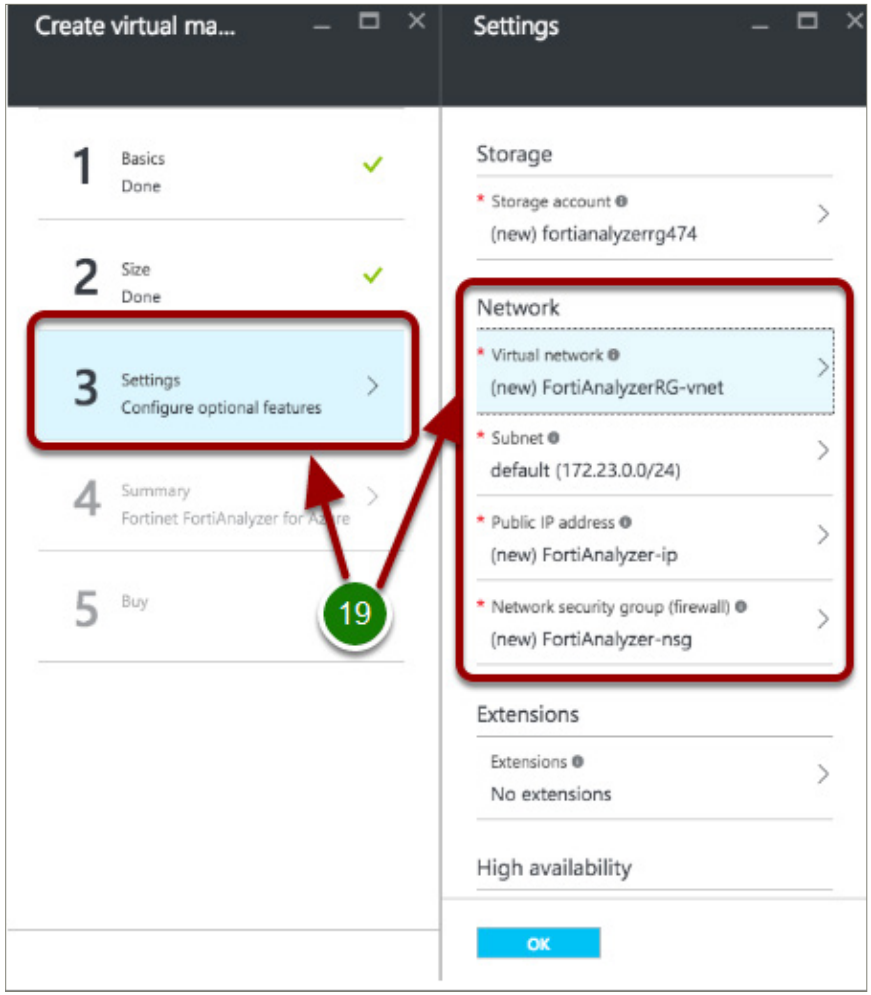
The data in the Azure Storage Account is always replicated in order to ensure durability and high availability. Be aware that some settings cannot be changed after the storage account has been created.

Select OK (18).

NOTE: No changes have been made here.

Configuring the FortiAnalyzer VM - Network

Network has several sub-tasks, which will be covered in sequence below (19).



Configuring the FortiAnalyzer VM - Network/Virtual Network

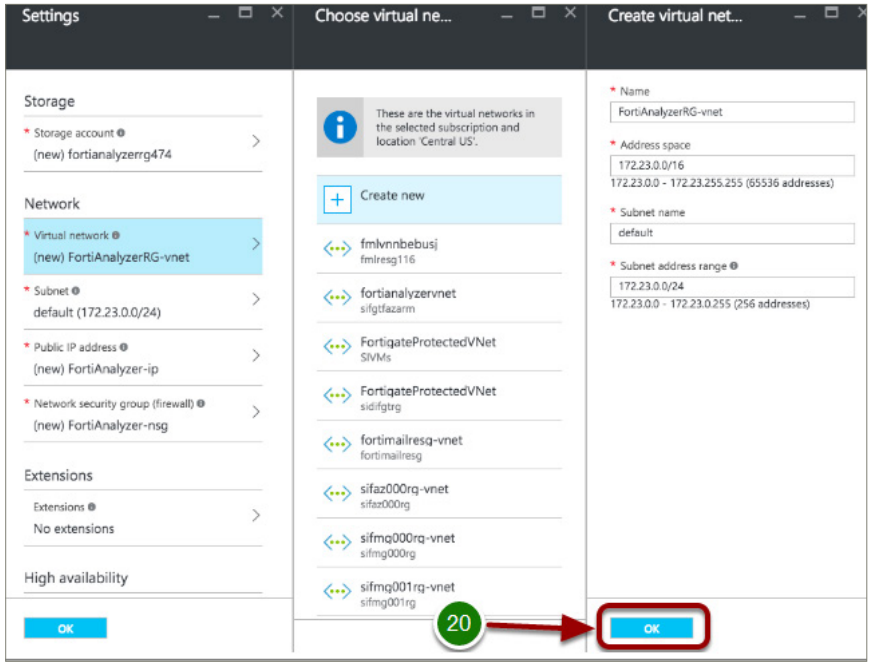
The first question that comes to mind about a virtual network (VNET) is why do we need a NVET? Well, the answer is a simple one and the basic principle here is that we need a VNET in order to be able to build a private network in the Azure cloud.

An Azure Virtual Network, which is also know or referred to as a VNET, is something that you only create in Microsoft Azure. The Azure Virtual Network enables virtual machines and the other resources that are part of the Azure Virtual Network to communicate with each other privately. It is the Azure Virtual Network that provides this communication function. If we did not have an Azure Virtual Network, or if a virtual machine was outside the Azure Virtual Network, then communication with other virtual machines would not be possible.

After you have selected the Virtual network settings, you will observe that you can either create a new virtual network or select an existing one. If you select an existing virtual network, it will need to have at least one subnet in order for the FortiAnalyzer to route. In a typical deployment, the “outside” subnet just connects the FortiAnalyzer outside interface to the Azure Public Load Balancer and therefore does not need to be very large.

Here we created the Virtual Network Name of FortiAnalyzerRG-vnet and the Address space of 172.23.0.0/16. Click OK (20).

NOTE: No changes have been made here.



Configuring the FortiAnalyzer VM - Network/Subnet

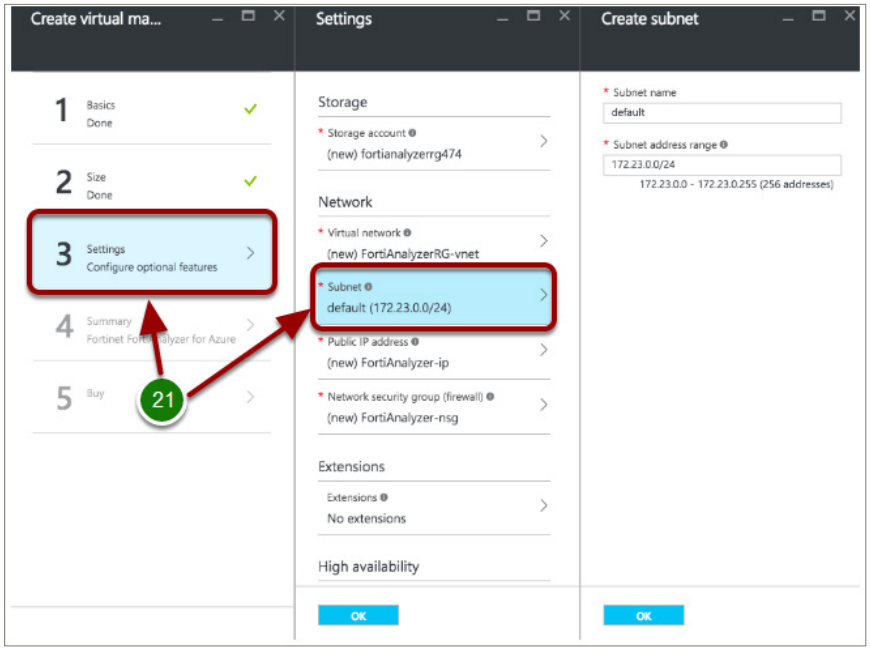
After you have selected the Subnet settings (21), you can also observe that we already have the following subnets defined:

Subnet name: default

Subnet address r: 172.23.0.0/16

So how does the IP addressing work? When a virtual machine is deployed into a VNET, its internal IP address is assigned from the subnet you specify and is dependent on the order in which it was provisioned, unless a static IP has been specified. For example, the FortiAnalyzer Subnet created uses the address prefix of 172.23.0.0/24. The first four IP addresses of each subnet are reserved. With this knowledge in hand, it is easy to deduce that the first IP address available in this subnet will be 172.23.0.5. Unless otherwise specified, a virtual machine will be assigned the next available IP address from the subnet to which it was assigned at provisioning time.

NOTE: No changes have been made here.

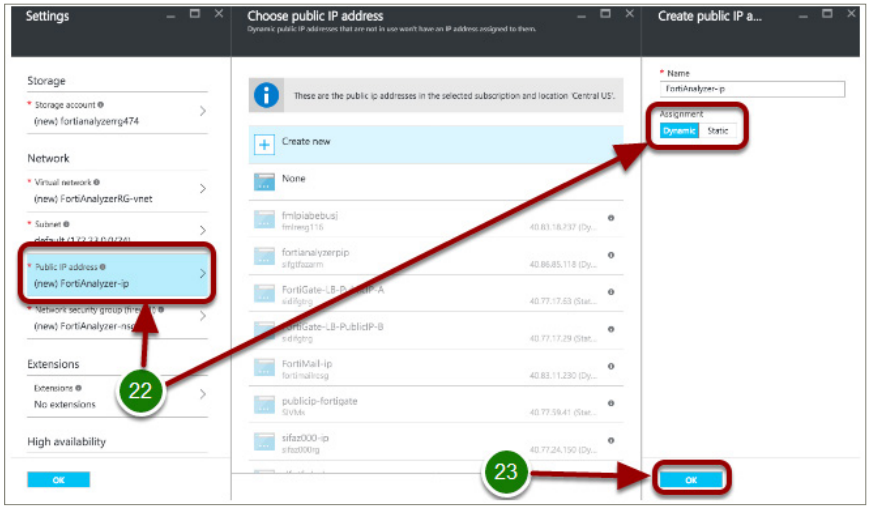


Configuring the FortiAnalyzer VM - Network/Public IP Address

Select the Public IP address settings (22).

Here you are just going to accept the default Name and Assignment Dynamic configuration and click OK (23). You could specify a static IP here within your subnet if you choose to do so.

NOTE: No changes have been made here.

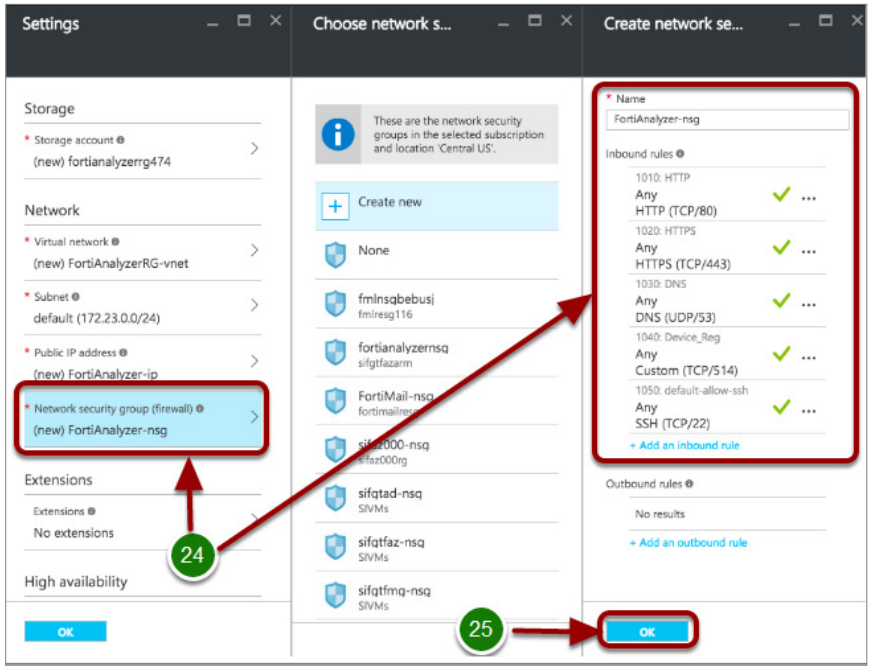


Configuring the FortiAnalyzer VM - Network/Network Security Group (Firewall)

Again we will leave the default Network security group (24); however, these are the predefined services allowed to the VM. Here you can Add an inbound rule or select custom security groups already defined.

Click OK (25).

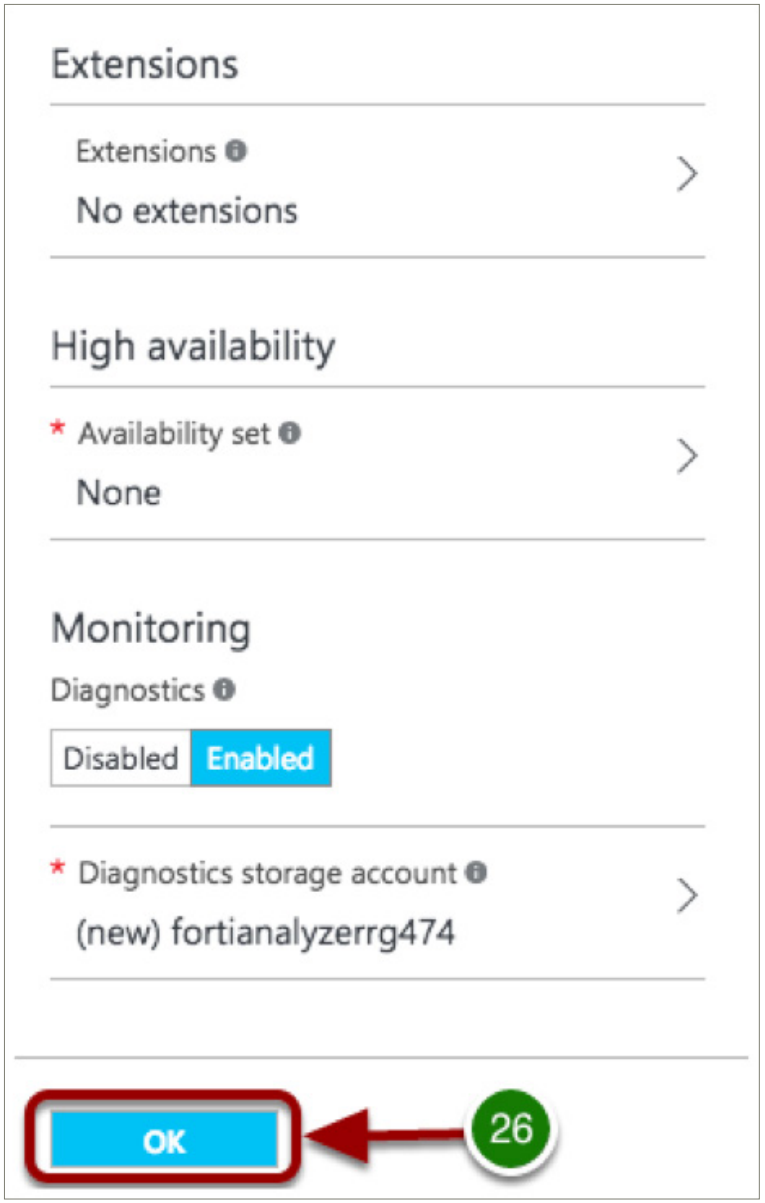
NOTE: No changes have been made here.



Configuring the FortiAnalyzer VM - Extensions/High Availability/ Monitoring

For purposes of this guide and deployment model, we will leave the defaults for Extensions/High availability/Monitoring (26).

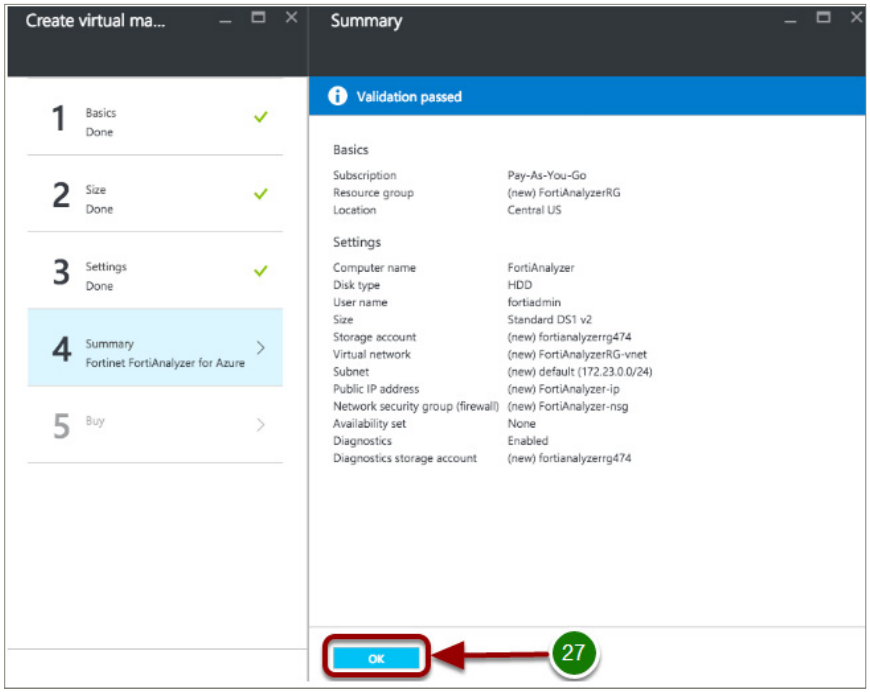
NOTE: No changes have been made here.



11. Configuring the FortiAnalyzer VM - Summary

    After selecting OK, a validation process will take place and your configuration will be validated. If successful, you will see Validation passed.

    Select OK (27).

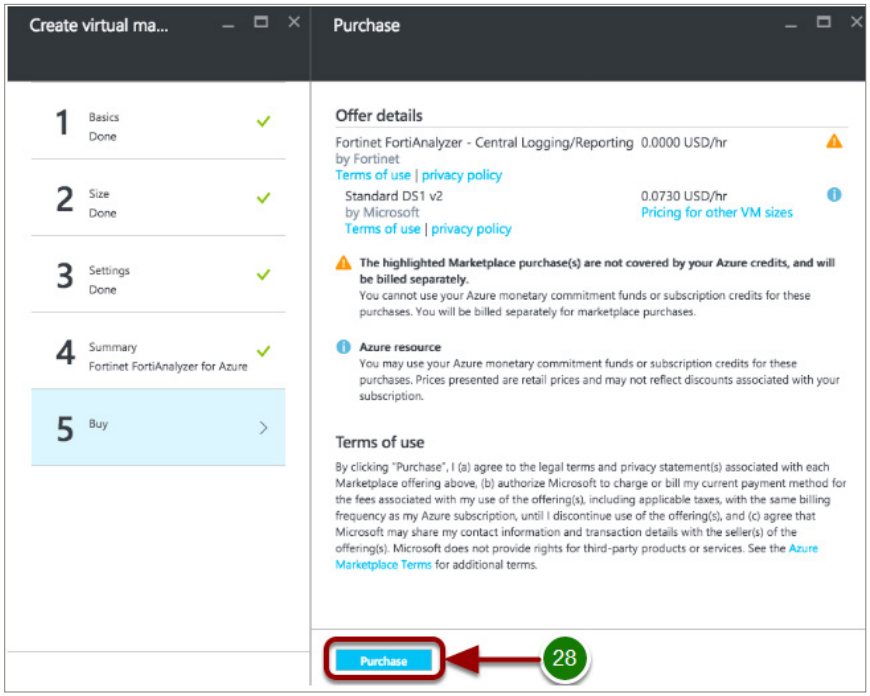


12. Configuring the FortiAnalyzer VM - Buy

    After the Fortinet FortiAnalyzer VM Configuration has been completed, you are now required to select “Purchase.”

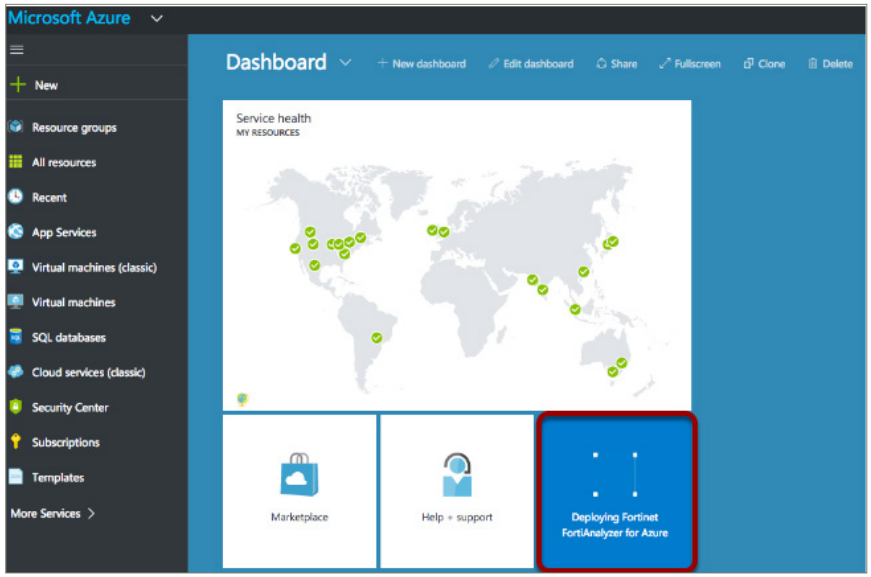
    Select Purchase (28).

    NOTE: Purchase just means that you are going to be paying Azure for the virtual machine use time. You still must obtain a license separately from Fortinet, Inc.



13. Fortinet FortiAnalyzer VM (Deploying)

    After selecting “Purchase,” the Fortinet FortiAnalyzer Single VM will be deployed. This process can take approximately 10 minutes to complete, but may vary depending on location and number of resources being requested.



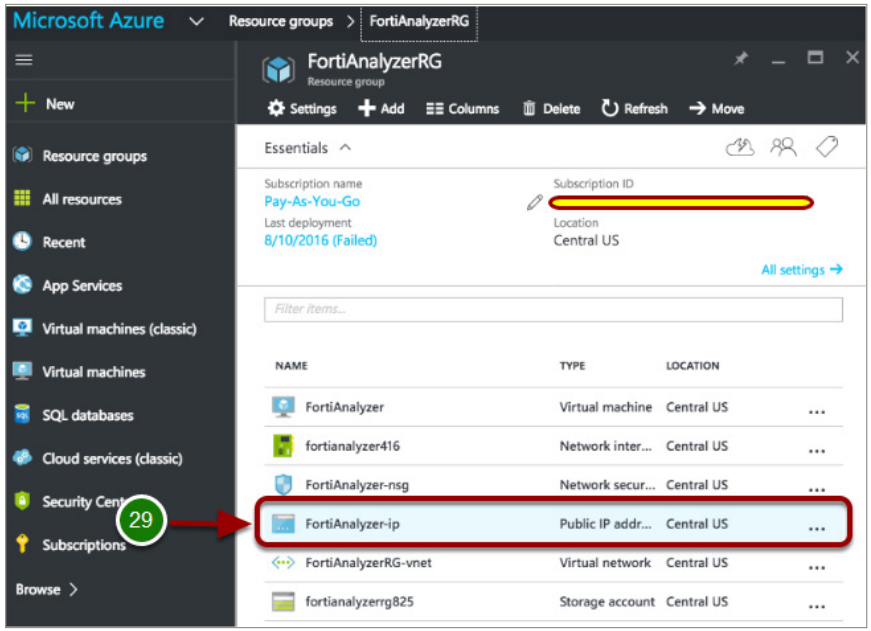
14. Connect to the FortiAnalyzer Azure VM by Public IP

    In order to be able to connect to the FortiAnalyzer Public IP Address, you need to know what this IP address is.

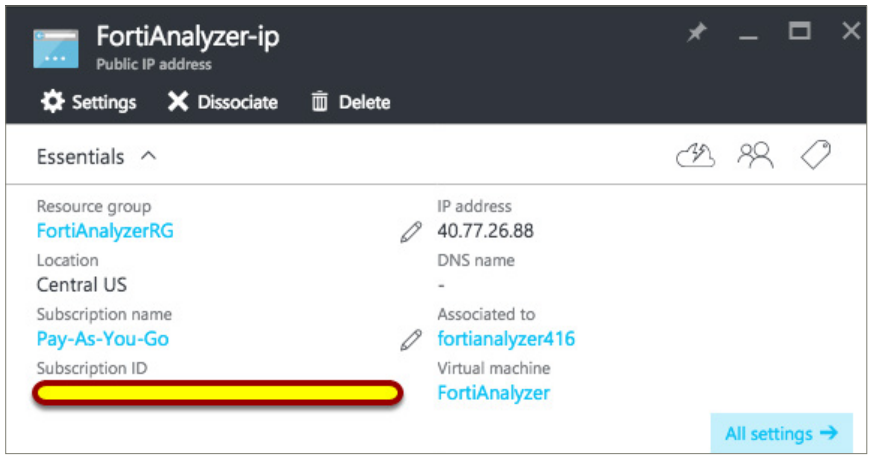
    To accomplish this:

    Once again from the FortiAnalyzerRG Resource group select FortiAnalyzer-ip (29).

    This will expose the public IP address, which is 40.77.26.88.



This will expose the public IP address, which is 40.77.26.88.



Connect to the FortiAnalyzer Azure VM by Public IP via SSH and Start LVM

SSH to the found public IP address, which is 40.77.26.88.

Recall in Step 8 you defined both the username and password, which are as follows and are required to connect to the FortiAnalyzer Virtual Appliance UI:

FortiAnalyzer Administrative Username: fortiadmin

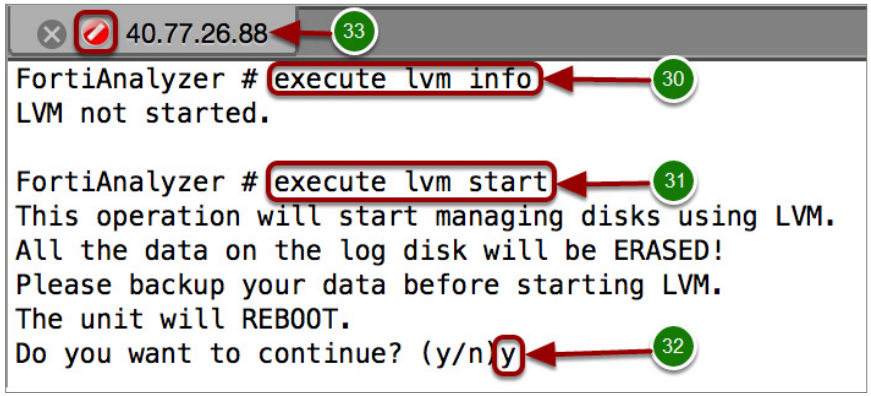
FortiAnalyzer Password: <the password you entered>

Type execute lvm info (30).

Type execute lvm start (31).

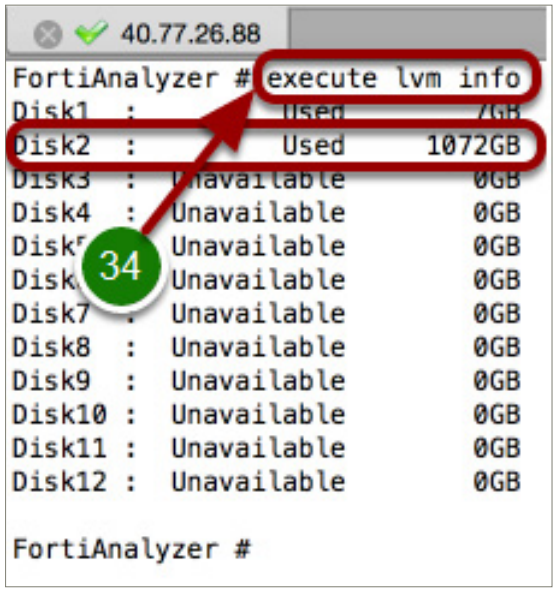
Type y (32).

FortiAnalyzer VM will reboot and SSH connectivity will go red (33).



Ensure you regain connectivity to the FortiAnalyzer VM after starting the LVM service. This could take a couple of minutes.

Type execute lvm info and verify LVM service is started and the newly created disk is attached (34).



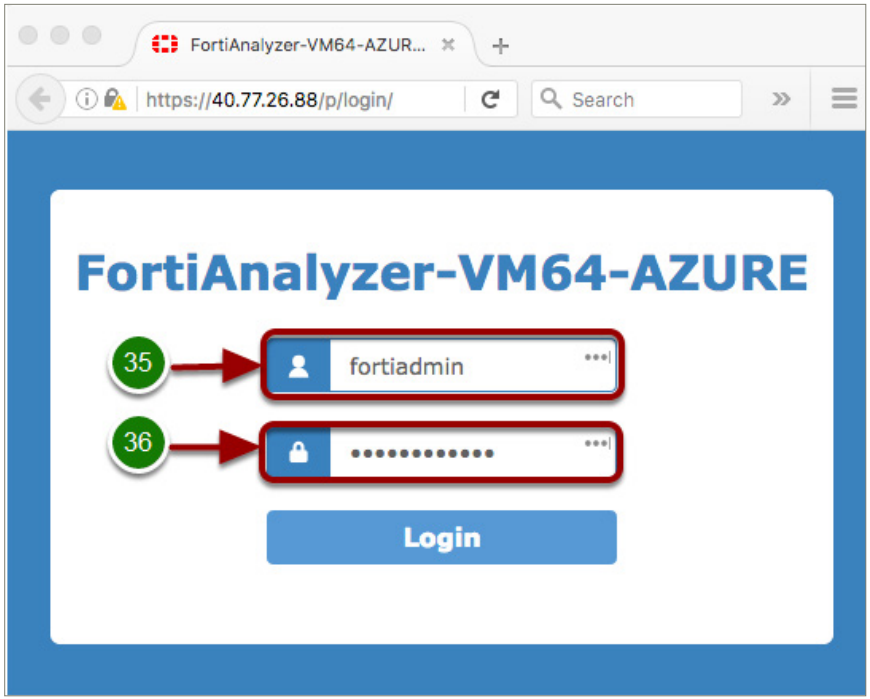
Connect to the FortiAnalyzer Azure VM by Public IP via HTTPS

HTTPS to the found public IP address, which is 40.77.26.88.

Recall in Step 8 you defined both the username and password, which are as follows and are required to connect to the FortiAnalyzer Virtual Appliance UI:

FortiAnalyzer Administrative Username: fortiadmin (35)

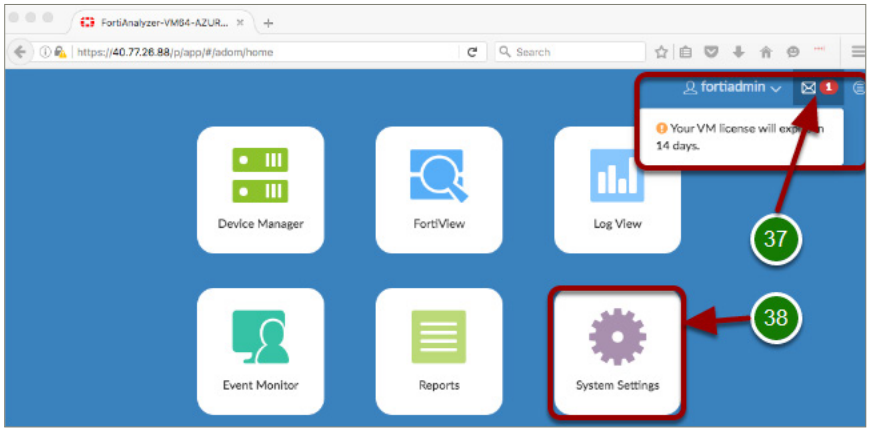
FortiAnalyzer Password: <the password you entered> (36)



15. Verify Temporary License - Check Messages

Click on your messages. You will see Your VM license will expire in 14 days (37).

Click on System Settings (38).



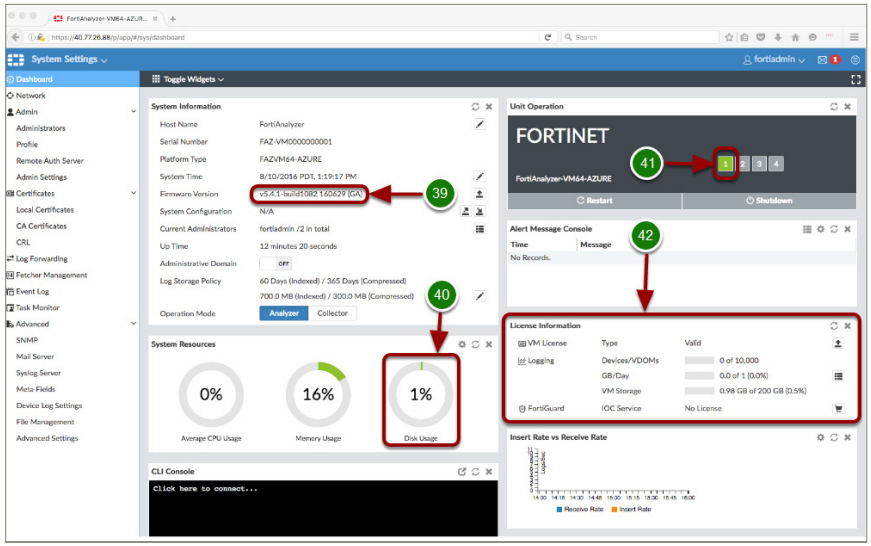
16. Verify Unit Operations - Firmware Version/Disk Usage/ Connectivity/License Information

    Firmware Version (39)

    Disk Usage (40)

    Connectivity (41)

    License Information—This is also where you would upload your BYOL obtained from Fortinet, Inc. (42)

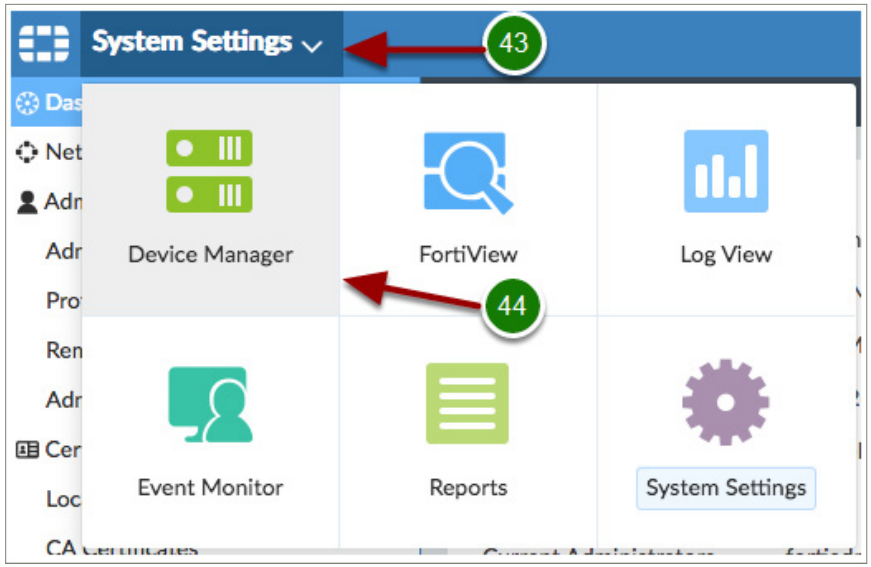


17. Navigate to Device Manager

    To navigate back out to the application selection menu:

    Click the System Settings drop-down (43).

    Click Device Manager (44).

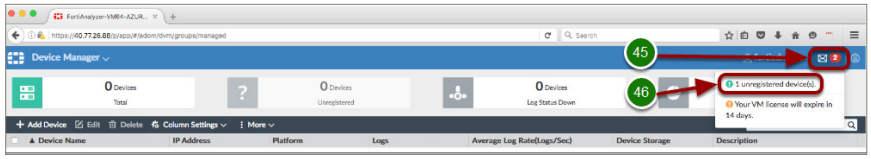


18. Add a Device

Once a device or FGT is pointed to your FortiAnalyzer Azure VM, you will be informed via a message.

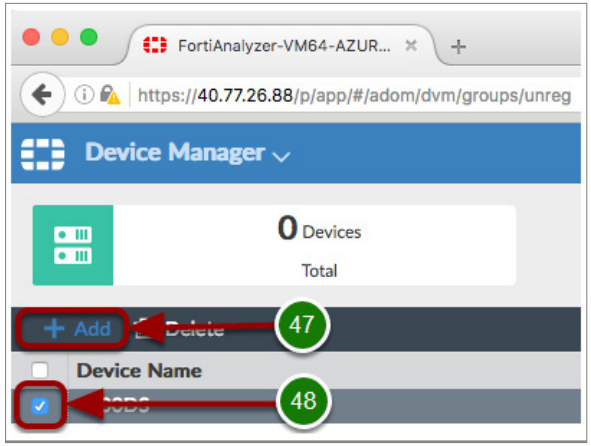
Click Messages (45).

Click 1 unregistered device(s) (46).



Click + Add (47).

Click the check-box next to your FGT Device Name (48).

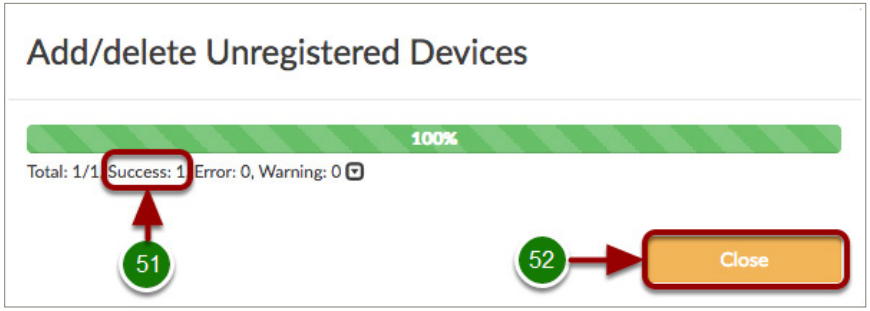


Enter the FGT name, Assign New Device Name (49).

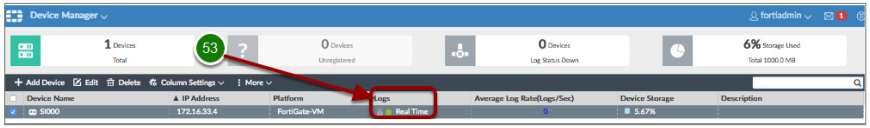
Click OK (50).

Verify Unregistered Device addition, Success (51).

Click Close (52).

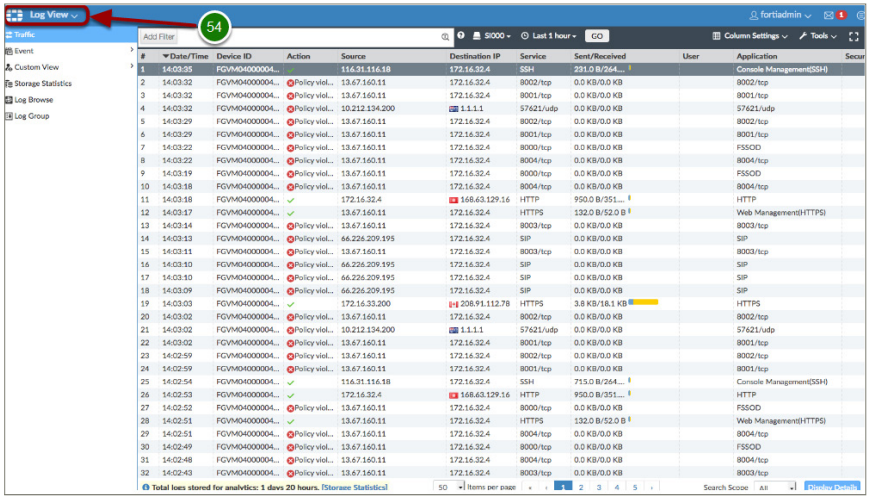


Verify Logs are being received, Real Time (53).



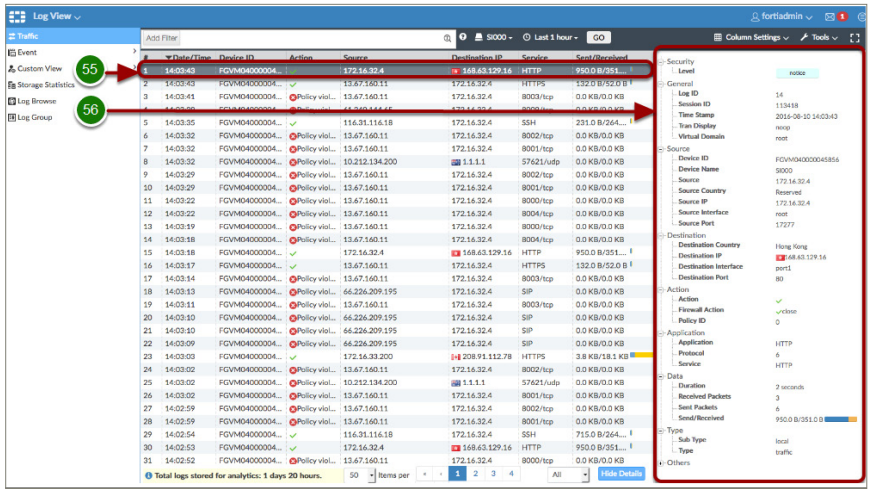
19. Log View

Navigate to Log View (54).



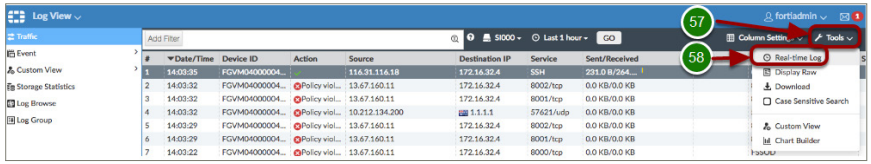
Single click any individual log to select it (55).

Double click any individual log to expand its Details (56).



To view logs scrolling real-time:

- Click Tools (57).
- Click Real-time Log (58).



20. FortiView

    Navigate to FortiView (59).

    Use the left pane to navigate through FortiView Summary, Threats, Traffic, Applications & Websites, VPN, WiFi, System, Endpoints, etc. (60)

Support

For more in-depth instructions, please refer to http://docs.fortinet.com/ for administration guides or email your support questions to azuretech@fortinet.com.

v1.0 09.07.16